

**What is claimed is:**

1           1.    A delegation method, implemented in a  
2 delegation system, comprising the steps of:

3           providing delegation policies as general rules for  
4           limiting delegation;

5           receiving a delegation condition and a delegation  
6           approval submitted by a grantor for vesting  
7           authority of the grantor's role to a grantee,  
8           wherein the grantor's role is designated the  
9           authority to access a set of data; and

10          determining consequent authority vested to the  
11          grantee based on the delegation approval, the  
12          delegation condition and the delegation  
13          policies.

1           2.    The method as claimed in claim 1, wherein the  
2 delegation condition is presented in extensible markup  
3 language (XML).

1           3.    The method as claimed in claim 1, wherein the  
2 delegation condition comprises a static condition for  
3 limiting the vested authority.

1           4.    The method as claimed in claim 3, wherein the  
2 static condition comprises at least a total time  
3 condition, a time condition, a location condition or a  
4 function condition.

1           5.    The method as claimed in claim 1, wherein the  
2 delegation condition comprises a dynamic condition for  
3 limiting the vested authority.

1        6.    The method as claimed in claim 5, wherein the  
2    dynamic condition comprises at least a session condition  
3    or a group condition.

1        7.    The method as claimed in claim 1, further  
2    comprising the steps of:

3        storing    the    vested    consequent    authority    as  
4                   consequent delegation information;  
5        creating    a    temporary    role    according    to    the  
6                   consequent delegation information using a role-  
7                   based system; and  
8        designating the temporary role to the grantee.

1        8.    The method as claimed in claim 1, wherein the  
2    determining step further comprises the steps of:

3        determining    whether    the    delegation    condition  
4                   satisfies the delegation policies;  
5        adjusting the delegation condition to the delegation  
6                   policies when the delegation condition does not  
7                   satisfy the delegation policies; and  
8        acquiring a consequent delegation condition, where  
9                   the consequent delegation condition comprises,  
10                  when the delegation condition does not satisfy  
11                  the delegation policies, the adjusted  
12                  delegation condition or, when the delegation  
13                  condition satisfies the delegation policies,  
14                  comprises the delegation condition.

1        9.    The method as claimed in claim 8, further  
2    comprising the steps of:

determining whether usage of the set of data satisfies the consequent delegation condition; and retracting the vested authority when usage of the set of data does not satisfy the consequent delegation condition.

10. A delegation device, comprising:

a memory storing delegation policies as general rules for limiting delegation;

a receiving unit for receiving a delegation condition and a delegation approval submitted by a grantor for vesting authority of the grantor's role to a grantee, wherein the grantor's role is designated the authority to access a set of data; and

a processing unit for determining consequent authority vested to the grantee based on the delegation approval, the delegation condition and the delegation policies.

11. The device as claimed in claim 10, wherein the delegation condition comprises a static condition for limiting the vested authority.

12. The device as claimed in claim 10, wherein the delegation condition comprises a dynamic condition for limiting the vested authority.

13. The device as claimed in claim 10, wherein the processing unit further determines whether the delegation condition satisfies the delegation policies, adjusts the

4 delegation condition to the delegation policies when the  
5 delegation condition does not satisfy the delegation  
6 policies, and acquires a consequent delegation condition,  
7 where the consequent delegation condition comprises, when  
8 the delegation condition does not satisfy the delegation  
9 policies, the adjusted delegation condition or, when the  
10 delegation condition satisfies the delegation policies,  
11 comprises the delegation condition.

1 14. The device as claimed in claim 13, wherein the  
2 processing unit further determines whether usage of the  
3 set of data satisfies the consequent delegation  
4 condition, and retracting the vested authority when usage  
5 of the set of data does not satisfy the consequent  
6 delegation condition.

7 15. A machine-readable storage medium storing a  
8 computer program which, when executed, directs a computer  
9 to perform a delegation method, comprising the steps of:  
10 receiving a delegation condition and a delegation  
11 approval submitted by a grantor for vesting  
12 authority of the grantor's role to a grantee,  
13 wherein the grantor's role is designated the  
14 authority to access a set of data;  
15 reading delegation policies as general rules for  
16 limiting delegation; and  
17 determining consequent authority vested to the  
18 grantee based on the delegation approval, the  
19 delegation condition and the delegation  
20 policies.

1        16. The machine-readable storage medium as claimed  
2        in claim 15, wherein the delegation condition comprises a  
3        static condition for limiting the vested authority.

1        17. The machine-readable storage medium as claimed  
2        in claim 15, wherein the delegation condition comprises a  
3        dynamic condition for limiting the vested authority.

1        18. The machine-readable storage medium as claimed  
2        in claim 15, wherein the delegation method further  
3        comprises the steps of:

4        storing the vested consequent authority as  
5        consequent delegation information;  
6        creating a temporary role according to the  
7        consequent delegation information using a role-  
8        based system; and  
9        designating the temporary role to the grantee.

1        19. The machine-readable storage medium as claimed  
2        in claim 15, wherein the determining step further  
3        comprises the steps of:

4        determining whether the delegation condition  
5        satisfies the delegation policies;  
6        adjusting the delegation condition to the delegation  
7        policies when the delegation condition does not  
8        satisfy the delegation policies; and  
9        generating a consequent delegation condition, where  
10       the consequent delegation condition comprises,  
11       when the delegation condition does not satisfy  
12       the delegation policies, the adjusted  
13       delegation condition or, when the delegation

14                   condition satisfies the delegation policies,  
15                   comprises the delegation condition.

1           20. The machine-readable storage medium as claimed  
2 in claim 19, wherein the delegation method further  
3 comprises the steps of:

4           determining whether usage of the set of data  
5           satisfies the consequent delegation condition;  
6           and

7           retracting the vested authority when usage of the  
8           set of data does not satisfy the consequent  
9           delegation condition.